

Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry

Verhage, Antoinette

Postprint / Postprint

Zeitschriftenartikel / journal article

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:

www.peerproject.eu

Empfohlene Zitierung / Suggested Citation:

Verhage, A. (2008). Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry. *Crime, Law and Social Change*, 52(1), 9-32. <https://doi.org/10.1007/s10611-008-9174-9>

Nutzungsbedingungen:

Dieser Text wird unter dem "PEER Licence Agreement zur Verfügung" gestellt. Nähere Auskünfte zum PEER-Projekt finden Sie hier: <http://www.peerproject.eu> Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.

Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

gesis
Leibniz-Institut
für Sozialwissenschaften

Terms of use:

This document is made available under the "PEER Licence Agreement ". For more Information regarding the PEER-project see: <http://www.peerproject.eu> This document is solely intended for your personal, non-commercial use. All of the copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public.

By using this particular document, you accept the above-stated conditions of use.

Mitglied der

Leibniz-Gemeinschaft

Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry

Antoinette Verhage

Published online: 26 November 2008
© Springer Science + Business Media B.V. 2008

“Whoever fights monsters should see to it that in the process he does not become a monster”- Friedrich Nietzsche, Beyond Good and Evil. Prelude to a Philosophy of the Future, 1886

Introduction

Money laundering, the ‘*process in which assets obtained or generated by criminal activity are moved or concealed to obscure their link with the crime*’ [12], has increasingly received attention during the last 20 years, from both policy makers and international organisations. This criminal phenomenon is depicted—first by the US, but followed by European countries—as a major threat to society and its economy. As a result, the battle against money laundering has become an international priority and—as some claim—a convenient motive for policymakers to implement far-reaching regulations and guidelines. This battle not only focuses on the prevention of money laundering as a crime in itself, but is also used as a means to identify the perpetrators of predicate crimes being the origin of the crime-monies to be laundered.

In the fight against profit-oriented crime and money laundering a large number of actors are involved, working on the prevention and detection of money launderers, based on a system in which public and private institutions on a national and international level cooperate. Prevention, detection and reporting are carried out by private partners, while the public partners have an analytic and repressive task. As a result of these international and national initiatives that were taken in the fight against organised crime and money laundering, we are currently witnessing the development of two parallel angles around the fight on money laundering and its

A. Verhage (✉)

Department of Criminal Law and Criminology, Research Group Social Analysis of Security,
Ghent University, Ghent, Belgium
e-mail: Antoinette.Verhage@UGent.be

predicate crimes: a legislative, regulative angle, designed to prevent and detect money laundering on the one hand, and an intrinsic commercial position towards anti-money laundering, stemming from a self-protecting reflex by financial institutions, aspiring to protect themselves against regulatory and reputational risks. These developments will be referred to respectively as the anti-money laundering (AML)-complex and the compliance industry. Between these separate and yet intertwined perspectives, we see private financial institutions, straddling both worlds. These private institutions are on the one hand a part of the AML complex, through the employment of inspectors who need to enable the institution to comply with the regulation: the compliance officers. On the other hand, however, these financial institutions purchase services from the—non-financial—compliance industry to support their implementation of AML measures, and are in this sense sponsors of the compliance industry.

The basic research question of our on-going research project is whether these (three) structures can be identified and in case of identification, how they function.¹ We aim to clarify this question by focusing on a specific type of actors within financial institutions that, in our view, are a good example of this bridge between the AML-complex and the compliance industry: the compliance officer. This article represents the first phases of this research and can therefore only provide a preliminary insight into the world of anti money laundering professionals. However, we should also note that the first phase to a large extent confirmed the research question. First we will discuss the research questions and the underlying theoretical assumptions that form the fundamentals of this research, after which a first empirical analysis of these assumptions will be described.

The anti-money laundering complex—origins

The battle against money laundering finds its origins in the United States in the late eighties, with the criminalisation of money laundering in 1986 [19]. Contrary to the rhetoric surrounding the “follow the money strategy” (fighting organised crime), the interests underlying the implementation of legislation and regulation against money laundering are not as uniform as they may seem. Several documents refer to the ‘war on drugs’ as the major force behind the anti money laundering legislation², but this was not the only push-factor for the invention of—what later became—a global ‘security quilt’ [15], focused on the prevention of what is referred to as “the flow of money from the illegal into the legal financial sphere”. Moreover, when analysing the years in which the anti-money laundering movement started, we see several other interests that support the commencement of this anti money laundering complex.

¹ ‘The anti-money laundering complex: an empirical research on the AML complex and its interactions with the compliance-industry’ UGent, funded by FWO Vlaanderen, 01/01/2006 – 31/12/2009

² E.g. THONY, J., Money Laundering and Terrorism Financing: An Overview, paper IMF, 2000 (www.imf.org/external/np/leg/sem/2002/cdmf/eng/thony.pdf), but also several policy documents relate the battle on money laundering to drug-related organised crime, for example FATF Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering, December 1988.

The “war on drugs”

In order to understand these diverging interests, we need to go back to the US in the 1980s, the period of ‘Reaganomics’: a deregulation of the economy and a tough-on-crime-policy [9]. In this period, the concerns over the profitability of crime and more specifically, drug crime, rose. The US government was concerned over the increasing threat of organised crime—personified by the mafia—and the threat of infiltration in both the legal economy and at political level [23]. Large sums of money were said to be in control of criminal elements, the underground economy was expanding widely [17], and policy makers concluded that traditional methods were no longer effective in fighting these forms of crime [22]. Hawdon states that this period can be characterized by a moral panic regarding the ‘war on drugs’ [9]—in fact the same rhetoric that was used by Nixon, when he used the war on drugs as a key issue in his election campaign in 1968 [7].

These concerns result in the Drugs Trafficking Offenses Act and the Money Laundering Control Act of 1986, through which money laundering becomes a criminal offence. The idea behind this new legislation was twofold: firstly, policy makers were convinced of the fact that crime should not pay. Secondly the ‘follow the money’ philosophy, focusing on seizure and confiscation of crime-money was identified as the best way to ‘hit them where it hurts most’ [18].

Financial interests

Parallel to these increasing governmental concerns, the 1982 financial crisis again pointed out how vulnerable the economy is. Central Banks took steps to protect the economy. One of the initiatives they proposed was the prevention of money laundering [11]. In their view, money laundering, apart from a profitable way to use illegally gained money in the legal economy, also has an impact on a broader macro level. To be more specific, it disturbs the normal flow of money within the financial system. In this view, the unpredictable money flows entering the legal financial system as a result of money laundering allegedly impact on the overall volume of money circulating within an economy [1]. These monetary volume changes supposedly disrupt the economy and have an influence on inflation, interest rates and exchange rates. Next to these concerns, money launderers, when they actually invest their illegally earned proceeds in the legal economy, also have an advantage in relation to the other (legal) players on the economic market as they are able to invest their illegally earned money in the formal economy; money laundering therefore results in unfair competition [24]. As Central Banks are responsible for ensuring a balanced monetary policy [10], they also have an interest in ensuring that this balance is not disturbed by unstable and destabilising flows of money.

Central Banks already were united in the Basle Committee since 1975, but based on these concerns they engaged in the battle against money laundering and presented a circular in 1988 on ‘the prevention of criminal use of the banking system for the purpose of money laundering’ [2]. In this circular they explained how banks can become victimized by money laundering, which can have several disturbing impacts, ranging from reputational damage, loss of public confidence in banks, or material damage as a result of fraud. The circular presented a statement of ethical principles for banks, based

on customer identification, compliance with laws and regulation and cooperation with law enforcement. Although private banks had previously been able to avoid stricter regulation on money laundering under the show of dishonest competition [17], when the Financial Action Task Force (FATF) was founded in 1989, and issued the 40 recommendations in 1990, such regulation could no longer be averted.

The EU directive in 1991³ introduced these anti money laundering standards to the European sphere, aiming at the coordination and cooperation of anti money laundering, but also indicating several obligations for all partners in the framework of a preventive approach of money laundering. These obligations referred to, inter alia, the identification of clients, the implementation of anti money laundering procedures and the duty to report suspicious transactions. Subsequently, member states were obliged to implement these European guidelines.

Reputational interests

Besides the legal framework surrounding anti money laundering, several initiatives were taken by the banking sector to protect themselves from fraud and from being used as a mechanism for criminal purposes. Self-regulatory initiatives related to corporate governance and reputation protection were put in place. The Wolfsberg group is one of many examples. This group of internationally orientated, large banks, developed a number of principles, the Wolfsberg principles (2000), which serve as a voluntary code of conduct for banks worldwide. These principles aim to harmonise compliance-, AML regulations and KYC rules, and encourage banks to exchange information on these subjects [19].

Apart from this initiative, the banking sector itself has extended the AML policy by forcing other banks to implement these measures in order to enable them to stay in the market [11]. Banks that do not follow this legislation are known in the sector and are seen as less stable and less healthy. Reputation is stated to be one of the most important factors in the financial sector and can therefore be used as a mechanism to put pressure on the sector. In particular the large, internationally orientated banks, working with many clients, government institutions and international organisations, are very much aware of the reputational and regulatory risks related to poor anti money laundering standards [16]. In other words: taking anti money laundering measures can also serve as a marketing tool. The question is to what extent the anti money laundering paradigm is still taken into consideration by the financial institutions when implementing compliance measures.

The irony of the implementation of AML measures is in fact, that banks are in se not harmed by allowing money laundering (passively or by rendering services). Money laundering in itself does not damage commercial interests or pose any financial risks. Therefore: without legislation, penal law enforcement and the accompanying reputational hazards, no commercially oriented bank would bother to prevent money laundering: criminal money is ‘cheap’ money for banks as these clients probably won’t ask too many questions and will not try to grasp all discounts. The harm derives from the fact that laundering is prohibited. There is an anti money laundering legislation put in

³ Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

place which results at least in reputational harm when a bank gets caught money laundering, or—even worse—is seen as associated with terrorist financing.

Since the AML-battle has now put severe strains on banks, the reputational risk (and following from this, the impact on profit-making) has become too high to take. The emphasis on the allegedly detrimental effects money laundering may have on the social and economic level has resulted in raised expectations from the legislator as well as from the public at large (as a result of the emphasis on corporate governance, ethical businesses etc), who expect banks to obey to these rules. As a result, money laundering has become one of the liabilities a bank has to deal with. But it is one with a high visibility effect which does not need to correspond fully with reality. This is endorsed by findings from the survey of PriceWaterhouseCoopers in 2007: 12% of all companies involved in the survey perceived money laundering as a high risk to their organisation. However, only 4% of these companies actually reported having experienced incidents related to money laundering [20]. The perceived threat of money laundering (or rather, the perceptions of its negative derivatives like reputation damage) is therefore higher than the actual occurrence. This is a good illustration of the impact of threat images, whether fanning crusades against organised crime [7], laundering, drugs, let alone a combination thereof.

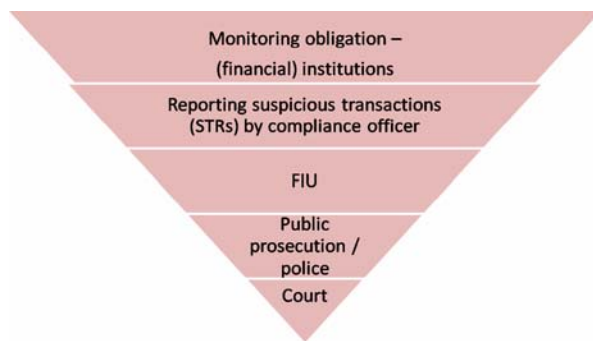
The war on terror

After 9/11, anti money laundering initiatives were lifted to a more severe dimension. After the war on drugs, now the War on Terror is a reason to implement far-reaching measures on anti-money laundering as terrorist financing is added to the AML Legislation. Before 9/11 governments had tried to implement client-profiles and ‘know your customer’ regulation. But this was stopped by the lobby of the banks and privacy-lobbyists [15]. The Patriot Act, however, implemented in the aftermath of 9/11, overruled these objections and introduced the possibility for information exchange between banks, but also enforced a larger access to that bank information for police and judicial services. Levi states that it would have been very unlikely that measures as intrusive as customer due diligence would have been accepted this silently without the attacks on 9/11 [15]. Moreover, not only were more comprehensive regulations introduced, the War on Terror also increased budgets for police and judicial services and broadened their competencies [13]. Banks chose to intensify their checks and procedures, as any association with terrorism financing could have disastrous effects [13]. The FATF developed specific guidelines for financial institutions to enable them to detect terrorist funding and the emphasis now shifted from drug related crime to all serious forms of organised (international) crime [8] and terrorism.

The Belgian implementation of anti money laundering legislation

After the elaboration of the international framework surrounding money laundering above, we will now focus on the Belgian implementation of the AML complex.

Belgium implemented the European guideline by means of the Law of 11 January 1993 on the prevention of the use of the financial system for money laundering. This law provides a preventive approach to money laundering and, in overall terms, implements the obligations of the EU Council Directive. In practice, this means that several

Fig. 1 The AML chain

organisations and/or persons (in the end, in 2006, 30.500 to be exact) are obliged to report suspicious transactions to an institution founded by the law of '93: the Belgian Financial Intelligence Processing Unit (CTIF-CFI). The CTIF-CFI was installed as an administrative (and not a judicial) organisation to enable this institution to work independently and autonomously. This special status is based on the role it should fulfil as a filter of reports to the police and the public prosecution. In this respect, the CTIF-CFI can rely on an extensive professional secrecy, enabling it to operate with the strictest confidence to both sides (reporting institutions and police or judicial services).

The judicial follow-up is carried out by the magistrates and police officers who are employed by the CTIF-CFI. Their involvement also guarantees access to all necessary information (police and judicial records) required to investigate any report received by the CTIF-CFI. If the CTIF-CFI decides that there is enough reason to suspect that (an attempted) money laundering has taken place, they will report this to the public prosecutor, who will investigate the case. Fig. 1.

The anti money laundering complex in Belgium comprises both public and private organisations, cooperating to prevent and investigate the laundering of crime-money: (federal) police and public prosecution, the Belgian Financial Intelligence Processing Unit—FIU (CTIF-CFI), the COSC (Central Office for Seizure and Confiscation) and the supervisor of the Belgian financial sector, the CBFA (Banking, Finance and Insurance Commission). Besides the framework built by the authorities around anti-money laundering, private organisations make up a large part of the anti-money laundering chain since they are obliged to report suspicious transactions to the CTIF-CFI. These organisations are listed in the Belgian anti-money laundering legislation⁴ and can be either financial organisations (banks, insurance companies, investment companies etc.) or non-financial organisations, such as lawyers, guarding companies or casinos and dealers in high-value goods. Private actors are a part of the AML complex as they are supposed to contribute to the prevention and detection of money laundering, but also represent the beginning of the anti money laundering chain.

⁴ Law of 11 January 1993 on the prevention of the use of the financial system for the laundering of money and financing of terrorism, B.S., 9 February 1993.

The compliance officer as the centre of anti money laundering implementation in banks

In the current research the focus lies on the task that financial institutions fulfil in the AML complex. This focus is based on several observations: this sector is one of the largest providers of reports to the CTIF-CFI and the bank sector is known for its large investments in trying to comply with the anti-money laundering legislation. Moreover, the credit institutions take up a unique place in anti-money laundering legislation and implementation as they are legally obliged to appoint one of their employees as responsible for the implementation and application of the anti-money laundering law. The supervisor (the CBFA) extended this legal obligation in 2001 [4] and obliged financial companies to install a specific function that (among other tasks) supervises compliance of the bank, staff and clients with anti-money laundering guidelines: the *compliance officer*.⁵ *Compliance*, or literally ‘observance’ is the key issue in the involvement of private actors in the battle against money laundering and refers to the extent to which private actors are able to fulfil the demands that are imposed on them by anti-money laundering legislation and regulation. The compliance officer is at the heart of the anti-money laundering investments by financial institutions and therefore represents an important actor in the complex. In short, this compliance officer will check transactions made by staff and clients, give training to staff and superiors, investigate clients’ backgrounds when necessary and make reports to the CTIF-CFI whenever a client or a transaction seems suspicious or could be related to money laundering or the financing of terrorism. In order to fulfil this task, the compliance officer makes use of several tools, such as software, specific programs and information providers.

The compliance industry

The overview we have given before regarding the origins and growth of the AML complex, does not represent the only push factor in the development of anti-money laundering initiatives. We state as a hypothesis that this progress of anti-money laundering implementation is supported by a parallel influence related to a more commercial approach associated with reputation risk management. We label this second force behind the anti-money laundering evolution as the compliance industry. The compliance industry represents the *entrepreneurial* approach to anti-money laundering and compliance. This supply side of the market on compliance is built around a number of services that provide support for AML and compliance officers: software providers (to enable in-depth transaction monitoring), trade-information bureaus (for information on potential organisational clients), databases of high-risk individuals (to enable thorough checks of potential individual clients), advisors (such as KPMG or E&Y), but also the provision of training and education for staff or for compliance officers themselves.

The tendencies towards a strengthened control on integrity and ethics of companies result in the willingness of, but also the need for, companies to propagate their compliance, reliability and social responsibility. This willingness did not

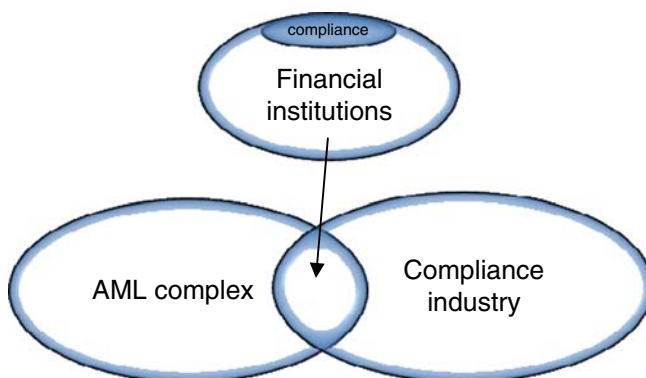
⁵ In some institutions, there are specific anti money laundering officers, working for the compliance department.

surface without any pressure; it took several scandals before companies realised the danger non-compliance can imply for their business and the harmful effects these scandals can have with respect to the company's image. The supervision from the US also plays an important role in this respect: without trust from the US supervisor, banks will not be able to work on the US market.

The compliance industry takes advantage of the need for an image of integrity and compliance and stimulates the demand for advice, support and software by advertising compliance as 'adding value to the business'. They stress the advantages of the implementation of compliance systems (such as transaction monitoring and know-your-customer-devices) by stating that this kind of information may also be used in a commercial manner. After all, having a large amount of information on customers enables the banks to offer tailor-made services and 'solutions'. The compliance-industry has grown extensively in recent years: estimations show that during the last years, banks (and other companies) have invested large sums of money in this kind of assistance and support [14].

Based on our finding that both trends act as parallel forces behind the enormous growth of the anti-money laundering movement during the last decade, in our research we are trying to find the perceptions of banks with regard to this global war on money laundering. As compliance and AML have become a market as well as a marketing product, we ask ourselves how banks perceive this development. And do they know what the results of their sizeable investments in compliance actually are?

Secondly, we aim to demonstrate that the compliance officer, as a partner in the AML complex, but also as a part of the compliance industry, functions between (and in) both worlds, and constantly balances the goals and interests of both worlds, alongside his in se dual function as an inspector in a commercial enterprise, having to make decisions that may sometimes go against the profit-making objectives of banks. This is the final part of the hypothesis to be elaborated in this article. Can we actually see the compliance function in banks as a bridge between both worlds? And does this mean that a compliance officer in practice continuously balances commercial interests and law-abiding goals?



Practice of the anti money laundering complex: KYC, CDD, monitoring and reporting

The anti-money laundering complex is coming into action within financial institutions by means of several measures. In our research question, the com-

pliance industry provides support for this implementation by offering advice and software.

Institutions under the AML legislation, burdened with the obligation to report suspicious transactions, are obliged to follow certain procedures in order to meet the requirements of the legislator. The Basel committee has made recommendations on the practical procedures [3], and the Belgian legislator has refined these guidelines. Legal requirements have been specified and refined in the Belgian anti-money laundering law and the Banking Law in 2007 [25], but also in the circulars of the regulator, the CBFA [4, 5]. In its 2001 circular, the CBFA had already defined the compliance function and listed anti-money laundering as one of the tasks of the compliance officer's mandate in the implementation of the integrity policy of the bank.⁶ The circular of 2004, updated in 2005, specifies the anti money laundering efforts a bank should implement. The first obligation in the 2005 circular relates to the development of a 'know your customer' (KYC) policy, and introduces a number of guidelines for identifying customers and beneficiaries of transactions. For example, this implies filing a copy of each client's identity card and mapping their background, family relations, business involvements, etc.

Furthermore, the circular details the procedures for accepting (new) clients, which also implies classifying clients by their 'risk rate'. Each client needs to be screened for the degree of risk they represent. 'High risk' clients are for example insufficiently identified individuals, or politically exposed persons (PEPs—individuals who may, because of their political status or otherwise, pose a higher risk for the bank). An example of a high risk transaction is a banking operation carried out by persons who are not identified by the financial institution itself, but by other institutions, which means identification takes place at a distance.

This risk assessment of clients automatically implies asking many questions in order to know the customer and his or her activities. This 'client due diligence' (CDD) also entails matching clients with the list of PEPs. According to the circular, PEPs can only be accepted after a thorough investigation of the person involved.

Related to this first phase in the implementation of AML guidelines regarding identification of customers and knowing their backgrounds, the monitoring (and subsequent investigation) of transactions is also detailed by the circular. The circular specifies the need for a *first-* and a *second* line supervision related to suspicious transactions.

The so-called first line supervision consists of the supervision carried out by employees who actually make contact with the clients through their daily activities. Specific employees, such as personnel working at the counters of banks, should be able to detect atypical transactions on the basis of predetermined criteria. After detection, they are required to report these transactions—in writing—to the compliance officer. The detection of these transactions needs to be based on the 'economic basis and legitimacy' of the transaction (why is this transaction carried out; why would this client make use of our bank for this purpose; does this transaction fit into the profile of our client; the amount of money involved in the transaction, the amount of cash,...). Banks are supposed to develop specific procedures for these routines.

⁶ This definition was subsequently included in the Banking Law in 2007.

The second line supervision consists of a ‘supervisory system’, a system which allows for the detection of atypical transactions of all accounts and transactions by customers. Every bank needs to develop refined, specific and pertinent criteria for the detection of these transactions. In addition, these criteria should be geared to the services and products the bank offers on the one hand, and to the clients they serve on the other hand. The formulated criteria should be connected to the risks related to money laundering or terrorist financing when dealing with transactions that, firstly, are carried out by high risk customers or, secondly, transactions that are atypical or raise suspicion regarding either the amount of money involved or when compared to the normal habits of the client. In order to fulfil this last demand, the system should be able to recognise ‘normal’ behaviour of clients and formulate a profile for their routine activities and transactions. This second line supervision is more detailed in the circular: it has to meet certain demands. For example, the system should produce written reports on the detected atypical transactions (‘alerts’), the reasons why these transactions are reported as atypical and, not unimportantly, it is supposed to be an *automated* system, unless the bank can demonstrate that this is not necessary [5]. This implies the development (or more often the purchase) of a monitoring device, which is often a type of software that allows for both monitoring and analysing transactions. This monitoring device needs to be examined for its pertinence on a regular basis.

After these two lines of supervision have resulted in several alerts, the circular states that the banks should analyse the alerts arising from both systems, ‘as soon as possible’. This is a specific task for the compliance- or AML officer. Banks are required to employ the necessary means and implement proper procedures to allow for an analysis of these alerts, as this analysis should result in a decision by the bank whether or not to report the alert to the FIU.

Apart from the obligations of the regulator with regard to the detection and reporting of suspicious transactions, banks are also subject to the obligation to train and educate their staff, which should enable them to detect and recognise potentially atypical transactions. Compliance departments are in consequence responsible for training employees in potential money laundering and terrorist financing methods.

These obligations result in rather detailed sets of measures a bank should take, although the criteria for assessing whether a transaction should be seen as atypical or even suspicious, remain rather vague. Both the KYC and the monitoring obligation imply the need (and in a sense the obligation) for making use of services provided by the compliance industry, supporting the implementation of AML measures. The market for AML monitoring software, for example, is relatively large, consisting of not only software providers that allow for the monitoring tool, such as *SAS* or *Norkom*, but also databases that allow for checking persons’ identities with several official lists to detect potential relations to terrorist groups or other high risk individuals. “*Worldcheck*” is one of the many examples. These services and software will probably be utilised further as the obligations imposed by the regulator keep rising. Furthermore, banks will also need to seek advice from professional advisors, such as KPMG or Ernst & Young to support the implementation of procedures and methods for anti money laundering activities.

Following this sketch of the origins, the current framework and the number of obligations that rest on the banking sector with regard to the implementation of anti

money laundering legislation and regulation, the second part of the article will discuss the practices and views of compliance professionals obtained from a survey of Belgian compliance officers.

The Belgian compliance officers

In order to get a primary, global view on this new professional group within the banking sector we made use of a quantitative method for gathering a basic level of information on compliance officers. In the spring of 2007, with the help of Febelfin, the federation of Belgian financial institutions, a questionnaire was sent via e-mail to their contacts on compliance.⁷ In the summer, the questionnaire was filled out on the Internet by 74 respondents. Since the survey was filled out anonymously and we do not know the exact size of the population we are studying, response rates are difficult to calculate. However, considering that the number of banks in Belgium was 104 at the time of the questionnaire, we may suggest to have gained at least a preliminary view on the compliance sector.

Despite the shortcomings of standardised questionnaires, such as low response rates, coverage errors and technical problems related to web surveys [6], we are of the opinion that the use of a web survey had several advantages. It allowed to reach a relatively large number of compliance experts in a short period of time. The goal of this web survey was to get a first impression of the backgrounds of compliance officers, their opinions and views on anti-money laundering regulation, cooperation and information exchange, but also to map different compliance practices⁸.

The next section presents the results of this questionnaire, related to the hypotheses above. First, a global view on the profession of a compliance officer will be portrayed, after which we will focus on the actual interpretation of the compliance function in Belgium, based on the results of the questionnaire.

Profiling the compliance officer

The first objective of the survey was to look for a profile of ‘the’ compliance officer. However, as soon became clear, there is no standard profile for a compliance officer. There are nonetheless some similarities as to the background of the respondents. For example, most of them are either economists or lawyers (or both), and have followed several additional courses or training in anti money laundering. The majority have worked for the banking sector for many years (or for another private corporation), although there are also compliance officers who have worked as a lawyer or have a

⁷ As compliance officers fulfil a discrete function within banks, they are hard to find. There are no contact addresses to be found on the internet, for example. Therefore, we needed an intermediary to get us in touch with compliance departments. Febelfin agreed to cooperate, but is not allowed to give out any addresses or names, which means the only way to get the questionnaire to the compliance sections, was to ask Febelfin to send them for us.

⁸ The results of this phase of the research will be used in the following, interview phase, which will be aimed at interviewing compliance and AML professionals from public and private institutions.

past in police, judicial, or regulatory institutions. Their age ranges from 28 to 63, with an average of 37 years of age, and the majority (70%) are men.

The majority of the respondents are employed by a large-scale, international bank (56%), while the others work for a small bank (26%) or an average-sized bank (15%). The banks are mainly based in Brussels.

Although their most common title is ‘compliance officer’, there are also compliance coordinators, heads of compliance, (chief) money laundering reporting officers, internal controllers, head legal and compliance etc. One of the explanations for this diversity is the fact that about half of the respondents are responsible for more than just the compliance task. One may wonder to what extent the combination of different responsibilities (such as the combination of legal advisor, or a senior position on the board, and the task of compliance officer), impacts upon the autonomy and independence of compliance functions. We actually see that compliance officers who combine the compliance responsibilities with other tasks, also have to report to two separate departments or persons. This could conflict with the independence of the compliance function in an organisation and put them in a difficult position, as it implies that ‘part-time’ compliance officers report to and are judged by a commercial entity regarding their tasks outside the scope of their compliance responsibilities. These functions entail a juggling of a commercial task and an AML task at the same time, which may lead to conflicts of interest. This observation is in line with the research question we have brought forward above.

Organisation of compliance departments in banks

We could derive from the survey that banks started organising compliance departments before it became an obligation. The large, international banks started to set up compliance departments in the late 1980s or early 1990s (although these were by no means exclusively linked to anti money laundering), while the small-scale banks waited until 1997 to introduce a compliance department in their organisation. By 2001 (the year in which the regulator obliged the introduction of a compliance officer), more than half of all Belgian banks in the sample had a compliance department at their disposal. A number of banks, however, waited to introduce a compliance department until 2003–2006. The internal organisation of compliance functions is not prescribed by the circular of the CBFA. Banks can decide for themselves which structure suits their institution best. This results in different choices by financial institutions: most of them (73%) opted for a centralised approach⁹ to compliance, which means that there is a central compliance department (in the head office, often in Brussels), combined with a national compliance policy (69%). This policy regarding compliance implementation varies: sometimes a degree of regional discretion is permitted, and in other cases, there is a compliance policy, specified for each business unit in the institution.

The compliance departments vary in size, related to the size of the bank, ranging from one single compliance officer to 75 people working in compliance. The size

⁹ In contrast to a decentralised approach. A decentralised approach implies the functioning of compliance units on a regional or local level, for example by use of ‘compliance antennas’.

has an effect on the hierarchy within the bank, but also on the level of responsibility that rests on one person or several persons. This is also reflected in the way in which they have to account for their compliance tasks: most of them make activity reports or have weekly meetings. Next to this day to day reporting most of them make annual reports or are assessed by use of certain quality criteria.

The majority of the compliance officers state that they are provided with sufficient powers and means to practise their compliance function and that their independence is guaranteed within the bank. However, this is the majority. One third of the respondents hold the opinion that they have insufficient powers and means to be able to perform their duties. These respondents may have a difficult time to implement anti money laundering actions in their bank, as a shortage of means may lead to a lower level of training, awareness and inadequate monitoring. This partly confirms the actual stressful relationship between commercial goals and compliance with regulation. On the other hand, the majority of the respondents state that their management *accepts* compliance investments, although not all of them state that management also *supports* compliance investments. This is also illustrated by the response to the question ‘a very stringent compliance officer will get into trouble with the management’, which was judged as ‘recognisable’ by one-third of all respondents. The balance between commercial and legislative goals apparently still needs to be found in some cases.

Compliance tasks

The circular of the CBFA regarding compliance prescribes several tasks as main responsibilities of the compliance function. In order to gain insight in the extent to which compliance tasks are actually related to anti money laundering we asked the compliance officers to what extent they perform these tasks on a daily basis. The result was a very diverse picture of task descriptions, leading us to suggest that the compliance function is a flag that covers different cargos.

Most of the respondents state that transaction monitoring is a daily task, together with the screening of clients and keeping up with legislation and regulation. However, we must emphasise the difference between respondents: some of them state that they never screen clients or stay up to date with legislation. On a less frequent basis, they perform tasks like making guidelines for employees, developing procedures and codes of conduct or providing training to personnel. Control functions are also performed on a frequent basis: controlling staff, investigating or reporting breaches of the internal codes, and reporting incidents to external parties are examples. A compliance function is not only a control function. On the contrary, a main part of the compliance officer’s task is to give advice. The advisory role is also emphasized in the regulation. This duality may be difficult to separate as employees may find it hard to ask advice from the same person that needs to check their actions and decisions. This could lead to a conflicting position within the organisation. Still, only a minority of the respondents felt that they functioned mainly as the banks’ police officer which could imply that they give priority to their advisory role.

AML in practice

What actually happens when a compliance officer suspects that a money laundering attempt has taken place or when funds that have entered the bank may be linked to

terrorist financing? The steps that are taken after suspecting a transaction, may shed some light on the functioning of the reporting system but also on the considerations that are taken into account when assessing a suspicious transaction. Most of the respondents state that the first thing they will do is to start their own investigation, complemented with performing a thorough screening of the client. Some respondents state that they will report this to the authorities immediately (without any research) or that they will contact a higher placed compliance officer. Only two of them state they will contact the client after receiving such a signal from an employee. Other possible actions they may consider are blocking the transaction if necessary, contact the employee in question or his/her office to get more information on the client and the transaction. One of the respondents stated: *“it depends on the type of transaction, but in order to avoid the risk of tip-off, we’ll choose to let the transaction proceed—but report it to the authorities afterwards”*.

In deciding whether or not to report a ‘suspicious’ transaction, several criteria are used. The most important criterion for compliance officers to actually make a report to the CTIF-CFI, is the background of the client: his or her precedents or previous suspicious activities. Secondly, the amount of money involved in the transaction is also important in assessing the suspicious nature of a transaction. When the transaction has crossed borders—international transactions—this may also be a reason to raise suspicion. Two other criteria that are important triggers for reporting are, on the one hand, the fact that similar cases were reported by the CTIF-CFI to the public prosecutor’s office and, on the other hand, when fellow-compliance officers advise them to report it. Of less importance is the relationship with the client, or the chance that reports will be taken seriously by the CTIF-CFI, although opinions vary on the latter: exactly the same number of respondents state that this actually *is* an important decisive factor. Other examples of standards used in assessing the suspicious nature of a transaction can be the relationship between the nature of the transaction and the profile of the client. This can give significant information: when transactions do not fit into the profile the bank has of a client, this is a reason to start asking questions. The same applies to the economic context of the transaction: are there specific reasons why this transaction should take place in Belgium, or through this particular bank? Some compliance officers also mention criteria such as the client’s age and the behaviour of the client during his visit to the bank. One of the respondents stated that reporting a suspicious transaction depends on the level of risk a transaction entails with regard to the banks’ reputation. This final observation reveals some of the conflicting interests that at work during assessing suspicious transactions. It may imply that reporting to the FIU function as an ‘umbrella’ for banks: when a report is made, a risk is covered. If there is no report, this is a calculated risk. In this sense, reporting suspicious transactions is a form of risk management. A well-considered risk management, as banks do not think little of reporting their clients to the FIU: half of the respondents stated that the suspicion had to be ‘very serious’ before they would report it to the FIU. In combination with the fact that a large part of the respondents estimated their reporting rate (the number of reports they make to the CTIF-CFI per year) as equal to or lower than other banks, we may assume that the reporting of suspicious transactions will only be carried out after the investigation has shown there are profound reasons for suspicion.

Based on these answers, our first conclusion is that reporting suspicious transactions can be seen as a well-considered strategy. Banks and compliance departments play their role in the AML complex, but in the mean time, they are very well aware of the risks involved and adopt their own strategies.

After sketching this more practical picture of the compliance departments, we think it is time to make an inventory of the visions of compliance officers regarding legislation and the impact of their battle against money laundering in general.

The compliance officer's perception of anti money laundering legislation

Many of the respondents state that the application of legislation and regulation has become too complicated compared to the year 2000. They point out that the current framework around the anti money laundering approach in Belgium has its shortcomings. One example of these shortcomings is the fact that anti money laundering legislation not only remains vague and open for interpretation, but also lacks focus on the most risky activities (one of the respondents explained this view by giving the example of the thorough checks on inland PEPs). Another example—and an obstacle that is often mentioned—is the level of feedback and information provision within the anti-money laundering complex. Feedback from the authorities, the police services, the regulator and the FIU seems to be quasi absent. About 80% of all respondents stated that there is a lack of information exchange between compliance and police services, and a large majority (90%) stated to be receptive for a more structural form of cooperation with the police services. The same applies to feedback from and information exchange with the regulator: the majority stated they would like to get more information from the regulator as to the way in which banks manage anti money laundering requirements. The FIU may function as another source of information in this respect, but also falls short of this demand. Compliance officers state that they need more information from the FIU with regard to their reporting obligations. From the open-ended questions we could deduce that the FIU usually does not give any clear answers when asked questions about suspicions. There is a feedback mechanism provided by the FIU, but this is limited to a quarterly feedback of all cases that were dismissed by the FIU. This means that, while the financial institutions are obliged to file reports, they have very little information (other than the standard criteria) on the basis of which they can decide whether to report to the FIU or not.

Banks and their compliance officers emphatically ask to be treated as partners in anti money laundering prevention and detection. This applies to all their contacts with the authorities. The respondents feel that banks, particularly compliance departments, are treated as suspects rather than as collaborators or partners during investigations. This is also emphasised by the fact that supervision by the authorities (the CBFA) is seen as sufficient—the chances of being caught are realistic according to the large majority. This gives rise to the interpretation that the AML complex is mainly a one-way street in which private actors need to invest, while receiving very little in return.

How can this relationship be altered? According to the respondents, a crucial aspect of a partnership with the authorities should be information exchange and access to certain kinds of information. Moreover, the compliance officers state that

the judicial authorities do not make enough use of the information provided by financial institutions.

Is AML a task for the private sector?

Do compliance officers think that they are performing an improper task, that actually is up to the authorities? One of the compliance officers stated that, in Belgium, all the responsibility for AML is unloaded onto the banks. Most of his colleagues agree: 77% think the government saddles the banking sector with governmental tasks. As banks are supposed to investigate any suspicion before reporting these to the FIU, the investments by banks in the AML implementation are rather high. Other respondents state however, that AML monitoring can only be carried out by banks, as an investigation by the bank is necessary in order to assess the level of suspiciousness. Some of the respondents stress the importance of this possibility to exercise discretion, in order to tailor their decisions to specific situations and circumstances.

Introducing reporting criteria

In relation to this demand for discretion, we need to remark on the recent changes in Belgian AML-legislation. In 2007, the legislator decided to introduce a number of indicators the banks should use in trying to assess whether a transaction is linked to organised and serious fiscal fraud. The introduction of these indicators is a political compromise: in the summer of 2007 there was a debate resulting from the ‘dematerialisation’¹⁰ of unregistered savings certificates, securities and bonds on the 1st of January 2008. As many of these savings are not fiscally known, banks accepting these funds could be guilty of cooperating with money laundering in the meaning of art. 505 of the penal code which relates to fencing (handling of stolen goods and money laundering).

To prevent this and protect bank employees, a law was accepted that had consequences on two levels¹¹. Firstly, article 505 was changed in the sense that only handling the proceeds of ‘organised and serious fiscal fraud’ in which complex mechanisms of international dimensions are used (as opposed to ‘common fiscal fraud’) falls within the reach of art. 505. Together with this amendment of art 505 of the penal code, a new article was introduced to the AML law of 1993: art. 14 quinquies, establishing 13 indicators for serious and organised fiscal fraud.¹² Banks (and all other reporting institutions) are obliged to use these indicators in assessing the suspicious nature of transactions. However, several weeks after this article 14 quinquies was introduced, a discussion started in Belgium on the compulsory nature of these indicators. The financial sector, the regulator and the FIU first stated that

¹⁰ This dematerialisation obliges clients to hand in their paper bonds to the banks – the ‘dematerialisation’ refers to the transformation from paper (‘material’) bonds to bonds posted in a securities account.

¹¹ Programmawet van 27 april 2004, B.S., 8 mei 2007

¹² The indicators can be found in the Royal Decree of 3 June 2007 – Koninklijk besluit tot uitvoering van artikel 14quinquies van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, 3 juni 2007.

these indicators should be used as *signals* for possible money laundering cases. However, the government gave a different interpretation to this article, stating that the moment *one* indicator is present in a case, banks are obliged to report the case to the FIU. The banking sector did not agree with this interpretation, stating that the indicators were too vague and may be present in many non-suspicious cases. They gave the example of international transactions (indicator nr. 9) or the absence of documentation to justify the bonds or savings (indicator nr 10). However, after the official governmental interpretation, the FIU was forced to adopt the same position.

The Belgian government justified the introduction of these specific reporting guidelines by referring to the reporting system of the Netherlands in which the number of reports is much higher than in the Belgian system. However, they apparently failed to notice that the Dutch legislator, after an evaluation of the reporting system, actually decided to abandon the system of objective indicators on money laundering reporting to a large extent. An evaluation of the Dutch system showed that a high number of reports does not automatically result in a higher effectiveness of the system [21]. It therefore at least surprising to observe the introduction of measures that were already found to be ineffective in another country.

Anticipating the introduction of these indicators in the Belgian AML system, we asked the compliance officers in our survey for their opinion on using specific guidelines for reporting suspicious transactions.

Concerning the introduction of indicators, 30 compliance officers stated that more specific indicators for reporting suspicious transactions would be welcome, while 14 respondents stated that on the contrary, more discretion was needed in deciding whether to report or not. Those wishing specific directions for reporting, justified their response by stating that this would lead to a more transparent system, identifiable cases of money laundering, more uniformity in reporting suspicions throughout the banking sector, or the limitation of grey areas on suspicious transaction reporting. Some stated that this would lead to more objective decision-making, and a better assessment of risks, as *“now the regulator judges arbitrarily whether we have taken appropriate action or not”*. The lack of information provision by the FIU is another justification for wanting more detailed instructions. Assessing whether a transaction is suspicious or not can be difficult, and help and feedback is welcomed in this respect. After all: *“the bank has no police investigative powers, and this is not the role a bank should play”*. It seems that the ability to use specific guidelines lightens the responsibility of banks by prescribing when to report or not, which implies that banks are more able to cover and calculate their risks. This is a good example of the impact of the AML system on banks and their decision making process; as a result of a strict follow-up and ever-expanding rules, banks want to be able to limit their risks by making a sound judgement of cases and by assessing their reporting duty and risks. Now it seems as though they feel the sword of Damocles hanging over their heads every minute. This may lead to a counterproductive interpretation of the reporting system. Nonetheless, when asked directly, almost all respondents state that compliance does not necessarily equate to ‘cover your ass’.

The opponents of the introduction of specific indicators for reporting, however, stress the fact that introducing specific instructions can only lead to more formality and may result in automatic reporting without any substantive consideration of the case. *“More specific indicators lead to a rise in reports of clients that may be acting*

a-typically, but are not laundering money. Actual money launderers will know the indicators better than anyone and will make sure they will not apply to them". They call the indicators 'pointless' and state that they will have no impact whatsoever on the level of actual money laundering. This is an example of the window dressing-characteristics of the system. Having a high number of suspicious transaction reports, does not automatically mean the prevention or detection of a large number of money launderers. Introducing measures just to increase the number of reports, may only result in a widening of the gap between public and private actors within the AML complex, as the usefulness of the system is increasingly questioned by the private institutions.

Furthermore, compliance officers state that a thorough analysis of cases will always remain necessary. This should be left to the compliance departments, as the knowledge and experience as a result of years of reporting by the compliance sector, should be used for interpreting potentially suspicious transactions. This experience is more valuable in assessing transactions than *"any typology or badly defined rule"*. *"The compliance officer is best placed to carry out a first investigation and assess 'authenticity' of the transaction. Experience shows that criteria are not helpful in this respect. One needs a certain 'feeling', which is not supported by criteria"*. Indicators are likely to be too general, and will need to be refined for each business line, as money laundering risks can differ according to the business clients are working in. The current process is risk-based, which implies a need for discretion, insight and experience, but also the possibility to make certain decisions. Only half of the respondents thought that the introduction of indicators would result in more useful reports to the FIU.

Some compliance officers remark that the introduction of indicators will remove an uncertain factor for commercial employees on the one hand, but will also result in a heavier burden on the commercial structures within the bank. One of the respondents stated that in fact, when such burdens are placed upon the banking sector, the authorities should also provide the sector with the means to enable implementation of these measures.

The introduction of these indicators may be an indication—as our respondents stated above—that the government is still not convinced of the trustworthiness of the banks. But how can the AML-chain function when there should be a cooperation, but there is no partnership?

Compliance officers and their opinion on compliance and AML

Investment in compliance can serve several purposes. Not only may it prevent victimisation of the bank, it can also provide a competitive advantage. More than half of the respondents stated that there are ways the sector can cope with dubious practices by other banks. A bank that structurally ignores the rules and regulations on money laundering (for example by accepting clients that other banks refuse), can be handled differently by the banking sector. For example, banks may warn the sector about this specific bank, or will break off any relationship with the bank in question. A minority stated that they would report this bank to the regulator, and seven respondents stated that they would consider leaking this information to the press. These statements not only emphasise the self-cleaning capacity of the banking

sector, but also confirm the hypothesis that compliance investments can serve as a competitive tool. However, as we shall discuss later, compliance and AML investments may also result in a weakening of the competitive position.

Compliance as a contribution to the business

Related to our hypothesis on compliance officers as being an ambiguous function within the bank—a non-commercial function within a commercial context—we tried to assess to what extent compliance officers either support the anti-money laundering goals of anti money laundering legislation or whether they comply with this legislation for other reasons. We asked the respondents for their ideas on positive and negative impacts that compliance may have on the functioning of a financial institution.

One of the most important positive consequences of compliance functions is the protection that compliance offers against reputation risks. Prevention of negative newspaper reports or other reputation damages (such as lawsuits or regulatory fines) are of major importance in assessing the value of compliance departments. Compliance has added greatly to the awareness of these risks by both management and employees and can now be seen as an important way to manage and minimise the risks of a financial institution: “*Today, without compliance, a bank can no longer function*”.

The emphasis on risk management and loss-prevention also emerges from the weight that is attached to the preservation of integrity; a profound integrity policy will teach banks to focus on the healthy and therefore profitable clients, clients that pose no risks for the bank. As a result, the compliance department contributes to the strategy of the bank as a whole. Furthermore, as one compliance officer remarks “*organisations that have their risk management settled, will be remunerative and have a positive effect on the outside world*”. This image or appearance of a trustworthy and honourable institution is for many respondents an important *raison d’être* for compliance. The image of integrity, which should not only be apparent on the outside, but also perceptible on the inside of the bank, is also important for the banking sector at large. Compliance, as a contribution to reliability and integrity, is therefore a ‘good advertisement’.

Other positive elements of the compliance function are the pro-active involvement of compliance sections in developing new products, services or marketing activities of banks, but also the guiding and advisory role the compliance departments take up in financial institutions. Compliance has taught financial institutions to find a reconciliation between legislation and entrepreneurship. The merit of the compliance function precisely lies in the ability to transform regulation into new business opportunities, according to one of the respondents.

Furthermore, it is thanks to the efforts of compliance departments that employees are aware of the risks and are taught to handle these risks by respecting the internal and external rules and regulations. The emphasis on compliance in recent years has also resulted in the staff being now well informed, educated and trained in operational control and anti money laundering. In other words, professionalism within financial institution is enhanced through the introduction of compliance in banks. Only a minority of the respondents mentioned the prevention of cooperation or conspiring with criminal activities as an important consequence of compliance investments.

Compliance as a hindrance to the business

On the other hand, the compliance officers also state that compliance functions can have negative consequences. Although two respondents were convinced of the fact that compliance only has positive outcomes, the majority mentioned a number of drawbacks. For example, compliance “*can slow down the business*”, or scare clients off. Entrepreneurial and commercial activities can be hindered as a result of too many rules, formality or bureaucracy and may result in conflicts between compliance and sales functions. The jungle of rules and obligations that has emerged in the last decades makes compliance, according to several respondents, an essentially bureaucratic process, but also a process that may harm the development of commercial activities. It implies a heavy administrative burden and slows down commercial processes and decisions because of the time investment, excessive monitoring and disproportionate reporting for the sake of accountability. All of this has resulted in a certain ‘compliance weariness’ within banks.

These factors not only hinder short term profit maximisation, but also in the medium-term the implementation of compliance and AML measures leads to reduced profits. After all, AML compliance also entails lower sales figures and reduced turnover, a consequence of having to refuse customers—also the bona fide customers. One respondent nonetheless made the observation that a commercial decision without compliance interference may cost the bank more on a long term.

One of the compliance officers commented on the competitive role of compliance investments, which may have some *adverse* effects: the use of unequal norms or differences in procedural demands between banks can have a negative impact on the position of a bank with a strict compliance policy. Clients will shop around for the least strict bank, where less questions are asked and less checks are carried out, which results in a faster service. These banks will have a competitive advantage in relation to the stricter banks. The only way to tackle this form of unfair competition is to enforce regulations in a serious way. However, this may also have some side-effects: the banks’ fear to be accused of non-cooperation with AML legislation is high: some of the compliance officers state that the risk of being fined or losing their banking license has an important impact.

Compliance efforts may, on the other hand also have a *positive* outcome: some state that banks can only survive in the market when they have put several compliance procedures in place (which impacts on the competitive position in a positive manner—compliance as good advertisement). Investment in compliance seems to work in both ways: it may serve as an impetus but also as an obstacle for competition. This image is reinforced by the observation that the banking sector makes sure that banks who are known for not complying with regulation or legislation are dealt with one way or the other by the sector.

Making use of the compliance industry

A small part of our survey was dedicated to the services provided by the compliance industry: software, training and advice on AML and compliance. We asked the respondents whether they make use of these services and if so, which kind of software they prefer.

The result was a very diverse repertory of monitoring software, applied for several goals. The compliance officers report using software for screening blacklists of clients and suppliers (name matching software, of which WorldCheck was mentioned most frequently; FircoSoft is also often used), but also transaction monitoring software is used extensively. Examples are Norkom, SAS, Complinet and many others. In most cases, a combination of both kinds of software has been purchased by the bank. 15 respondents note that their bank has implemented 'in-house developed software', aimed at monitoring transactions. These banks are often smaller banks, as they are not able to make use of programmes supplied by a parent company (in contrast with the large banks, which have software at their disposal through the parent company). But also medium-sized banks may choose to develop their own software, to have a tailor-made programme, suitable for their activities. A small minority (4 respondents) state that they do not make use of any monitoring software.

In general, the respondents state to be satisfied with the software they have at their disposal, although some state they would like to have a name-matching programme.

Another dimension of the compliance industry is the provision of training and education for compliance and AML professionals. Respondents are positive about the supply of training on AML, although one third states that the supply of training possibilities is insufficient.

The final question related to the services of the compliance industry relates to the employment of expert advice on compliance and AML. These services are actually used: 57% of all respondents state that they hire external advisors (such as KPMG or Deloitte & Touche) occasionally, or on a regular basis. 43% states they have never made use of this service.

These results make clear that the compliance industry actually is a reality in the implementation of AML measures in financial institutions. Most banks make extensive use of the services provided by the compliance industry, which gives us not only an idea of the investments related to the AML system, but also shows how many interests (and thereby profits) are involved. However, the presence of software does not automatically imply a watertight system, moreover, it may serve as an alibi, showing the bank is actually investing in AML and complying with regulation, while it is the effectiveness of the system that needs to be questioned.

To conclude: the compliance officer between the hammer and the anvil?

After discussing the empirical results of the survey, we return to our initial research question. Is the compliance officer actually trapped between commercial goals on the one hand and rule-abidance on the other hand? We suggest that our research question is to a large extent supported by the results. However, we need to gain more in-depth knowledge of the day-to-day practice and issues of the compliance and AML professionals before we can indisputably answer this question. Nonetheless, taking the limitations of these first results into account, we may draw some preliminary conclusions. As half of our respondents stated that compliance remains a battle between commercial interests on the one hand, and rule observance on the

other hand, we conclude that the compliance function has an inherent contradictory characteristic. Although the respondents state that compliance as a whole is not limited to a ‘cover your ass’-policy, the thesis ‘the good reputation of the bank still comes first’ was unanimously answered with ‘yes’. This seems to imply that compliance mainly aims at preventing risks, but particularly reputational and regulatory risks (the risk of getting fined or excluded from operating in the sector), and not per se money laundering risks.

When we asked the compliance officers to list the most important goals of compliance (in their view), the two goals, unanimously endorsed by all respondents, were to prevent the bank from getting involved in criminal activities and the protection of the bank against reputational damage. The three goals that followed were 1) to comply with current rules and legislation (98%); 2) to support the battle against money laundering (94%); and 3) to know the clients’ backgrounds (84%). Although it remains important, we can deduct from this that fighting money laundering is not the primary goal of the AML efforts by banks. In this respect, we may ask ourselves to which extent the authorities’ policy of fighting money laundering is a goal in itself overlapping but not fully covering the mindset of the financial sector.

Most banks state that without government regulation, the efforts of the banking sector on the prevention of money laundering, would not be as high as they are today. According to the majority of compliance respondents, self-regulation by the banking sector would not lead to the same effects. This is in some senses surprising—as most respondents state that investments in anti money laundering serve a primary goal—reputation protection. This raises the question: why would this goal no longer apply when no enforcement is carried out in this respect? Or would reputation no longer be at stake when supervision is no longer present? Or is reputation concerning *money laundering* rather the product of threat image creation, while in normal circumstances the public would rate the bank’s reputation in terms of solvency and efficiency?

To conclude, the multiplicity of interests at stake in the whole of the AML system, makes it difficult to paint a clear picture of whose goals are achieved. The three angles involved in the battle against money laundering, result in a blurry mixture in which several benefits and concerns are muddled up;

- The AML complex on the one hand serves several goals (both the official goal—repression of crime—and the economic interests of several players).
- The compliance industry, on the other hand, strives for profits based on the implementation of AML measures and benefits extremely from each new kind of regulation or legislation. Moreover, we conclude that legislation has actually strengthened and consolidated the compliance industry by obliging banks to make use of their services. The AML complex and the compliance industry are mutually reinforcing constructions, and in this sense also preserve one another through this interdependence.
- The financial institutions, stuck between both of these angles, have their own concerns and motives for investing in the AML battle: reputational protection, preventing harm to the company and preventing regulatory fines. These interests drive the banks to the implementation of costly and intrusive measures in the battle against money laundering and terrorist financing, the involvement of a rather large amount of new AML-professionals and the introduction of high

standard instruments, purchased from the compliance industry. The ambiguous function of the compliance officer within the financial institution illustrates the difficulties related to this diversity of interests.

The question is to which extent these intertwined and contradictory interests result in a system that functions as either a self-fulfilling prophecy or as an alibi. Although it is a system with potential, the danger rests in preserving a system that can no longer be questioned as too many interests are at stake. The awareness of these interests is a first and necessary step in preventing the anti money laundering system from ending like Pygmalion or Narcissus: a system so blinded by the image it has created and by its own reflection, that it is no longer able to critically question itself.

Acknowledgements I would like to thank the editor of this special issue, Petrus van Duyne, for his critical, yet enthusiastic, comments to earlier drafts of this article. I also thank Paul Ponsaers, my promoter, for his guidance and advice and Marc Cools for his useful suggestions. Special thanks to Febelfin for their assistance and above all to the compliance officers who took the time to fill out the survey.

References

1. Bartlett, B. (2002). The negative effects of money laundering on economic development. *Economic Research Report*.
2. BCBS (1988). Prevention of criminal use of the banking system for the purpose of money-laundering: 4.
3. BCBS (2005). Compliance and the compliance function in banks: 16.
4. CBFA (2001). Circulaire D1 2001/13 aan de kredietinstellingen.
5. CBFA (2005). Gecoördineerde versie d.d. 12 juli 2005 van de circulaire van de Commissie voor het Bank-, Financie- en Assurantiewezen over de waakzaamheidsverplichtingen met betrekking tot de cliënteel en de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme.
6. Dillman, D., & Bowker, D. (2001). The web questionnaire challenge to survey methodologists. In U. Reips, & M. Bosnjak (Eds.), *Dimensions of Internet Science*. Lengerich: Pabst Science.
7. van Duyne, P. C., & Levi, M. (2005). *Drugs and money. Managing the drug trade and crime-money in Europe*. Oxon: Routledge.
8. Gouvin, D. (2003). Bringing out the big guns: the USA patriot act, money laundering, and the war on terrorism. *Baylor Law Review*, 55(101), 956.
9. Hawdon, J. E. (2001). The role of presidential rhetoric in the creation of a moral panic: Reagan, Bush, and the war on drugs. *Deviant Behavior*, 22(5), 419–445.
10. Hazlitt, H. (1979). *Economics in one lesson. The shortest and surest way to understand basic economics*. New York: Three Rivers.
11. Helleiner, E. (2000). The politics of global financial reregulation: lessons from the fight against money laundering. *Working paper 15*. Centre for Economic Policy Analysis and New School of Social Research.
12. International Monetary Fund (2004). The IMF and the Fight against Money Laundering and the Financing of Terrorism. A Fact Sheet.
13. Kochan, N. (2006). *The washing machine. Money, crime and terror in the offshore system*. London: Duckworth.
14. KPMG (2004). *Global anti-money laundering survey 2004*.
15. Levi, M. (2002). Money laundering and its regulation. *The Annals of the American Academy of Political and Social Science*, 582(1), 181–194.
16. Levi, M. (2005). Controlling the international money trail: what lessons have been learned? *Global Enforcement Regimes. Transnational Organized Crime, International Terrorism and Money Laundering*. Amsterdam: Transnational Institute (TNI).
17. Naylor, R. (2007). *Criminal profits, terror dollars and nonsense*. Tax Justice NL, Seminar on Money Laundering, Tax Evasion and Financial Regulation., Transnational Institute Amsterdam.
18. Nelen, H. (2004). Hit them where it hurts most? The proceeds-of-crime approach in the Netherlands. *Crime, Law and Social Change*, 41(5), 517–534.

19. Pieth, M. & Aiolfi G. (2005). Anti-money laundering. Levelling the playing field. Basel, Basel Institute on Governance: 48.
20. PriceWaterhouseCoopers (2007). Economic crime: people, culture and controls. The 4th biennial Global Economic Crime Survey.
21. Regeling indicatoren ongebruikelijke transacties (2005). Regeling tot hernieuwde vaststelling van een indicatorenlijst voor ongebruikelijke transacties 19 augustus 2005. Nr. FM 2005–00241 M.
22. Thony, J. (2002). Money laundering and terrorism financing: an overview, International Monetary Fund: 1.
23. Van Heuckelom, C. (2004). Het tot stand komen en de krachtlijnen van de Wet van 19 december 2002 tot verruiming van de bijzondere verbeurdverklaring. In J. Denolf, & E. Francis (Eds.), *Follow the Money. De jacht op crimineel geld* (p. 13). Brussel: Politeia.
24. van de Werdt, E., & Speekenbrink, P. (2008). Witwassen, een koud kunstje. In J. De Bruin, P. Diekman, R. Hoff, et al. (Eds.), *Jaarboek Compliance 2008* (pp. 201–216). Nieuwerkerk aan de IJssel: Gelling.
25. Wet van 22 maart op het statuut van en de toezicht op de kredietinstellingen (1993).*B.S.*, 19 April